# IAD Texas Department of Health
# Internal Audit Division

TDH

August 30, 2002

Eduardo Sanchez, M.D.
Commissioner of Health

Dear Dr. Sanchez:

This is the **REPORT OF OUR EXAMINATION OF THE DEPARTMENT'S PROGRESS IN PREPARING FOR COMPLIANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) - AUDIT REPORT #200212.** This is the second in a series of reports on this topic. Our examination showed the Department has made significant progress in preparing for HIPAA. The Department (1) completed a regulatory assessment and interpretation of the finalized rules and conducted a number of Department-wide HIPAA awareness presentations, (2) assigned responsibility for the HIPAA project to the Office of the Associate Commissioner for Information Systems and allocated the necessary resources without any line item state funding or federal reimbursement and (3) conducted an initial HIPAA risk assessment with additional supplemental assessments and completed a compliance action plan. Other actions include (1) hiring both a project manager and privacy officer, (2) developing a comprehensive HIPAA intranet site, (3) developing a Project Management Plan and a Communication Plan and (4) developing a cost estimate for four of six phases of HIPAA that are expected to be finalized in the near future.

## INTRODUCTION AND BACKGROUND

A major concern facing the healthcare industry including providers, health plans and information clearing houses both government and private is the ability to comply with HIPAA regulations. Enacted by Congress on August 21, 1996 as part of a broad attempt at incremental healthcare reform, HIPAA requires all healthcare organizations to comply with standards and requirements set by the United States Department of Health and Human Services (HHS) for the maintenance and transmission of all health information both electronic and manual. The main goals of the standards are (1) improve portability and continuity of health insurance coverage, (2) combat waste, fraud and abuse in health care insurance and delivery, (3) to improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for certain administrative and financial transactions and (4) to protect the security and confidentiality of all health care information. HIPAA regulations pre-empt all state regulations unless the state laws are more restrictive with some exceptions such as those for health plan auditing, licensure or oversight. Civil penalties for failure to comply include a $100 fine for each violation with a maximum penalty for all violations of an identical requirement not to exceed $25,000 in a year. Criminal penalties for wrongful disclosure of health information offenses may result in up to a ten-year prison sentence and $250,000 fine.

HIPAA is an enterprise-wide issue that will affect both information technology and business operations. Cost estimates to complete the project at the Department range from $8 to $10 million dollars, and will have to be accomplished without any direct State or federal line item funding. Additionally, compliance will require the Department change the way it conducts business. The implementation of HIPAA standards requires the careful evaluation of the legal, regulatory, process, security, and technological aspects associated with each rule. The process of implementing all sections of the HIPAA standards will take some time, and will require a long-term commitment from the Department. Two of the HIPAA standards have been finalized including Electronic Data Interchange (EDI) transaction standards, code sets, and privacy. The other ones are slowly being finalized throughout 2002 and 2003, each with two year plus two month implementation deadlines.

The HIPAA standards (rules) are broken down into nine parts each with different compliance dates. The first finalized rule was EDI transaction standards and code sets. Transaction standards specify how health care information will be formatted for electronic transactions. The code sets specify why patients are seen and the procedures that are performed. The Department previously used locally developed code sets that will require migration to the HIPAA specified code sets. The initial compliance deadline was October 16, 2002. However, the key system with which the Department interfaces is the new Medicaid Management Information System called Compass 21, and the systems administrator, National Heritage Insurance Corporation (NHIC), would not begin working on any design modifications to the system until a contract was in place to perform the work. The contract was finalized in May of 2002, which would not allow enough time to complete the project. The Department filed for and was approved a yearlong extension moving the compliance date to October 16, 2003 to complete the necessary work.

The second completed rule was Privacy, and the compliance date is April 14, 2003. The privacy rule covers all medical records. Furthermore, the 77th legislature enacted Senate Bill 11 which is more restrictive and further protects medical records. The privacy rule will have the biggest impact on how the Department conducts day-to-day business. For example, when health related statistical information is released it cannot contain any information that uniquely identifies a specific individual. This includes names, addresses, phone numbers and could even be the county of residence in some very small rural counties.

The final rules to be finalized include (1) security, (2) national provider identifier, (3) national employer identifier and (4) national health plan identifier. Three other rules are on hold including (1) claims attachments, (2) enforcement and (3) national individual identifier.
All finalized sections of HIPAA are published in the Federal Register and can be found on

the HHS web page, which has a direct link from the Department's HIPAA intranet site. The Department must continue the vigilance and level of effort that has been shown towards HIPAA in the future to ensure compliance by the required due dates for each of the last rules as they become final.

## SCOPE AND METHODOLOGY

The examination of the Department's efforts to comply with HIPAA is an ongoing effort. Our review was limited to the examination of records and surveying Department officials. The review was conducted in accordance with Generally Accepted Governmental Auditing Standards and the Standards for the Professional Practice of Internal Auditing.

## STATE-WIDE EFFORTS

The National Data Interchange Standards Task Force (NDIS or task force), established by the Texas 76th legislature and presided over by Texas Health and Human Services Commission (HHSC), has been assigned as the advisory body for HIPAA's implementation and a forum for the exchange of information. The role of NDIS was expanded by the 77th legislature to include integrating the provisions of HIPAA, preparing a financial analysis and assessing the State's overall progress in implementing HIPAA. The task force has established a HIPAA Project Management Office (PMO) and a project director.

Currently, the PMO is assisting the operating agencies (TDH as well as other identified agencies) and NHIC in completing a HIPAA Gap Analysis, mapping EDI transaction sets to current data, reviewing and mapping local codes and drafting a Medicaid Privacy Client Notice. Additionally, the PMO is drafting the NDIS Task Force Report as required by the legislature. Although HHSC is assisting, the responsibility for funding, staffing and completing a total HIPAA compliance project in a timely manner is the responsibility of the Department.

## DEPARTMENT EFFORTS

The Department has made significant progress in preparing for HIPAA compliance. A regulatory assessment and interpretation of the two finalized (EDI and Privacy) rules has been completed with the help of the Legal staff at the Department and HHSC. A Fit/Gap analysis is in progress for the EDI standard. The Privacy Fit/Gap has been assembled to identify the various aspects of the rule that the Department must address. Beginning in May of 2001, the Department has conducted 19 HIPAA awareness programs including presentations, outreach and education. The different programs were designed to meet the needs of the varied target audiences including the entire Department, region staff, Department Management, program management and providers.

Responsibility for HIPAA was assigned to the Office of the Associate Commissioner for Information Systems who hired both a Project Manager and a Privacy Officer. The

Department has allocated the necessary resources from an extremely tight administrative budget, which was significantly reduced for FY2003, to progress this far with the project. However, if the Fit/Gap analysis for the EDI standard reveals the need for major programming changes or compliance with the upcoming Security standard requires a major hardware investment, it is unclear if the Department will have the necessary resources to comply with HIPAA. Neither the State nor Federal Government has provided any direct funding to complete the project.

A Department-Wide HIPAA survey was sent out in May of 2001 to all areas within the Department. The survey indicated the HIPAA EDI standard might affect 61 programs. A second survey was distributed in September to further refine the HIPAA impact analysis. The survey results revealed 42 programs would be affected by the standard. Furthermore, the Department is a hybrid agency containing both plans and providers. For example, the Health Steps Program at the central campus is a plan since it provides no direct patient services. However, in the regions where Department staff actually provide the services, the program is a provider.

Since the 9 rules are all finalized at different times, the initial Privacy assessment survey was sent out separately in February 2002. Survey results indicate that 61 programs will be affected by the Privacy rule. However, Senate Bill (SB) 11 of the 77th State of Texas Legislature governs the privacy of health information and provides for more coverage than HIPAA. Both HIPAA and SB 11 will be implemented at the same time due to resources and the overlapping nature of the legislation. A second privacy survey has been distributed to address the bill which has a compliance date of September 2003. Initial estimates are that all but a handful of the 204 programs at the Department will be governed by the privacy requirements outlined in SB 11.

The Department has formulated a compliance action plan. The plan includes key documents such as the (1) HIPAA Project Charter and Amendment, (2) Project Management Plan, (3) Communication Plan, (4) detailed task listing (overall as well as EDI and Privacy individually), (5) compliance timeline for security and privacy, (6) critical path document and (7) HIPAA Cost Accounting & Tracking Plan. Several EDI specific items include (1) the diagramming of all the affected areas computer systems and all external interfaces with those systems and (2) the formation of a local code workgroup to map the state local codes to the new national code sets. All of the project documentation is located on the Department intranet under Agency Projects/HIPAA.

## CONCLUSIONS AND RECOMMENDATIONS

HIPAA is a far-reaching piece of legislation with substantial penalties for noncompliance. The Department has made significant progress toward the implementation of HIPAA. However, the lack of direct funding for a project of this size, which to date has been funded from the existing budget, places the successful implementation of HIPAA at a high level of risk. The Department should be commended for its efforts to-date considering this large obstacle.

We recommend that the Department continue the implementation with the level of effort it has shown to date.

We will continue to monitor the project as critical dates are reached through the end of 2003.

## MANAGEMENT COMMENTS

Management agrees with the report.

Sincerely,

Mark Scott, CPA, MBA
Director, Internal Audit